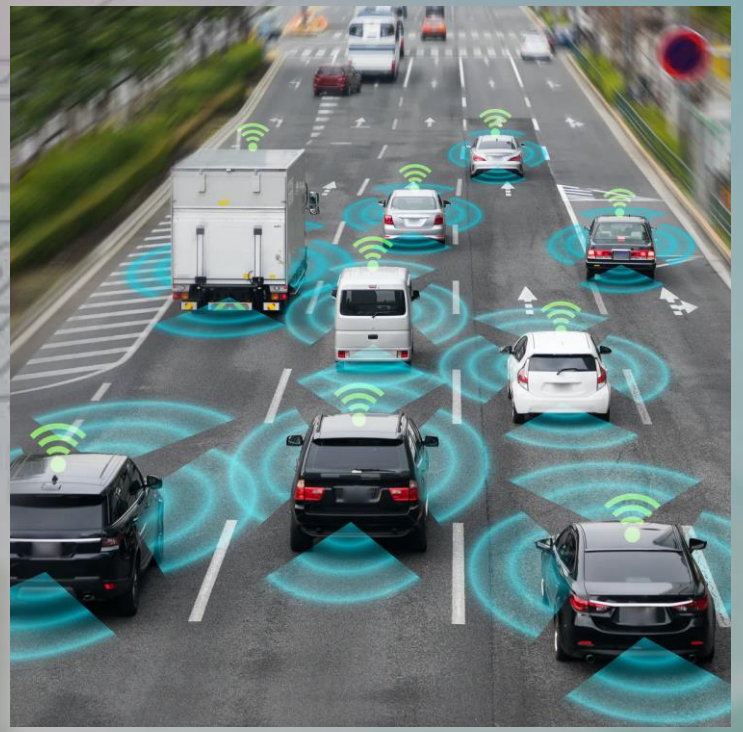
TNO innovation for life



SAFETY AND SECURITY CHALLENGES FOR COOPERATIVE, CONNECTED AUTOMATED MOBILITY (CCAM)

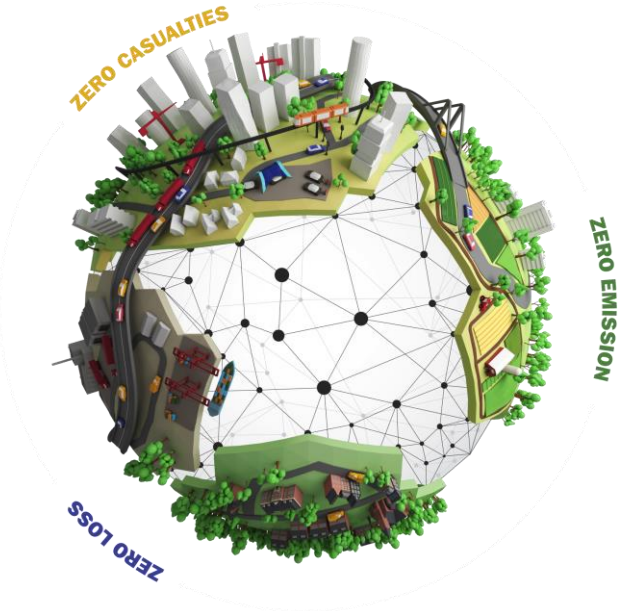
FRANK BENDERS

INDEX

SAFETY AND SECURITY CHALLENGES FOR COOPERATIVE, CONNECTED AUTOMATED MOBILITY

TNO innovation for life

INTRODUCTION
GOAL IN AUTOMOTIVE



ZERO LOSS:

- Reduce the number of hazardous accidents
- This requires using complex cyber physical systems to avoid collisions

ZERO CAUSALITIES:

- Reduce the number of traffic jams and transport delays
- This requires using traffic information and advance automation using the cloud and maps and GNSS (GPS)

ZERO EMISSION:

- Use bio-fuels/electric suspension where need/possible
- Increase efficiency of transport flows
- This requires using GNSS and map data for smart charging and planning of fuel switching

INTRODUCTION
GROWING NEED FOR MOBILITY

CITIES

- Urbanisation → Growing population → Scarcity of space, healthy environment, energy

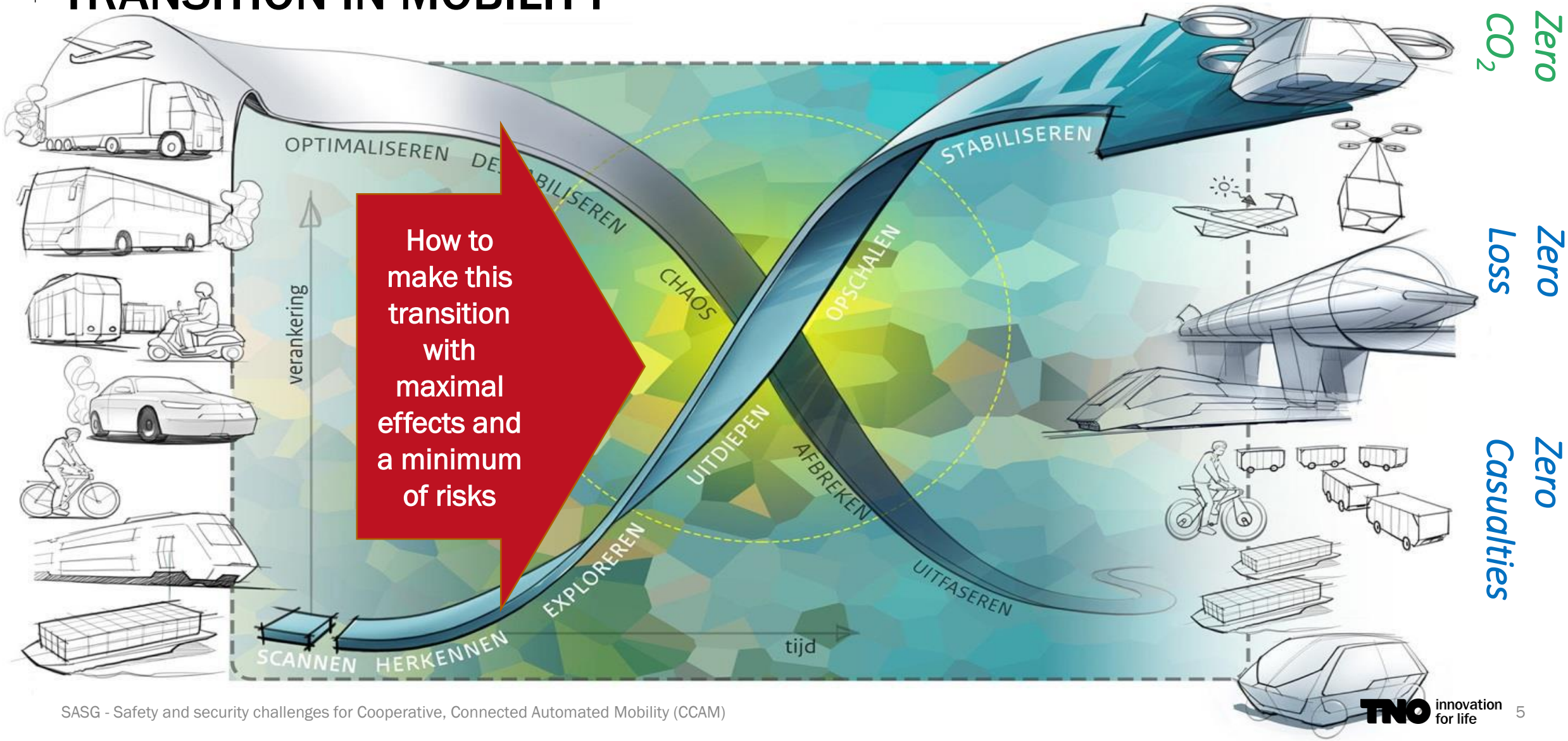
LOGISTIC HUBS

- Complexity → ICT, automated vehicles, and logistics & need for efficiency

CORRIDORS

- Globalisation and growing dependency on (digital) infrastructures → increased interoperability and standardisation

INTRODUCTION
TRANSITION IN MOBILITY



INTRODUCTION
COOPERATIVE, CONNECTED AUTOMATED MOBILITY

CCAM

- Possible solution for the complex dilemma

Challenge

We have a growing need for mobility and transport	We aim for Zero Casualties, Zero Emissions And Zero Loss

Example applications:

- Platooning
- Intelligent Speed Advice
- Road Works Warning
- Smart Intersection Crossing
- Green Light Optimisation Speed Advice (GLOSA)
- Infrastructure Supported Automated Driving

INTRODUCTION

TRENDS IN AUTOMOTIVE – CCAM

- **Development knowledge**: Combined System/Safety/Cybersecurity Engineering + Model Based Engineering
- **# Computers:** Hybrid computers ECU/CPU/GPU
- **Software**: Distributed multi-threaded software (millions lines of code)
- **Autonomy**: Transition to automated (SAE L3-L4) → Autonomous (SAE L5)
- **Networks**: Multi-layered network + including many smart gateways + Hybrid network and several Cloud/Fog
- **Sensors**: Many distributed/remote sensors
- **Redundancy**: Double/triple redundancy for safety and security reliability
- **Liability/Responsibility**: Vehicle Manufacture + Suppliers become responsible in case of casualties
- **Data storage**: Distributed and remote data storage
- **Privacy**: Private in vehicle/Cloud/Fog data – including data encryption
- **Update/maintenance**: Over the air updates and remote support/maintenance
- **Navigation**: Local/distributed/cloud based map information (High Resolution + sensor dependent map info)
- **Standardisation**: Increasing number of standardised message and protocols in automotive (WiFi-p / 5G)

TECHNOLOGIES
KEY ENABLERS

ENABLING TECHNOLOGIES

- Smart sensors
- Connectivity (Wifi-p, 5G/6G, etc.)
- Blockchain, advanced cryptography (including post-quantum cryptography)
- Digital platforms
- Artificial Intelligence
- Internet of Things (IoT)

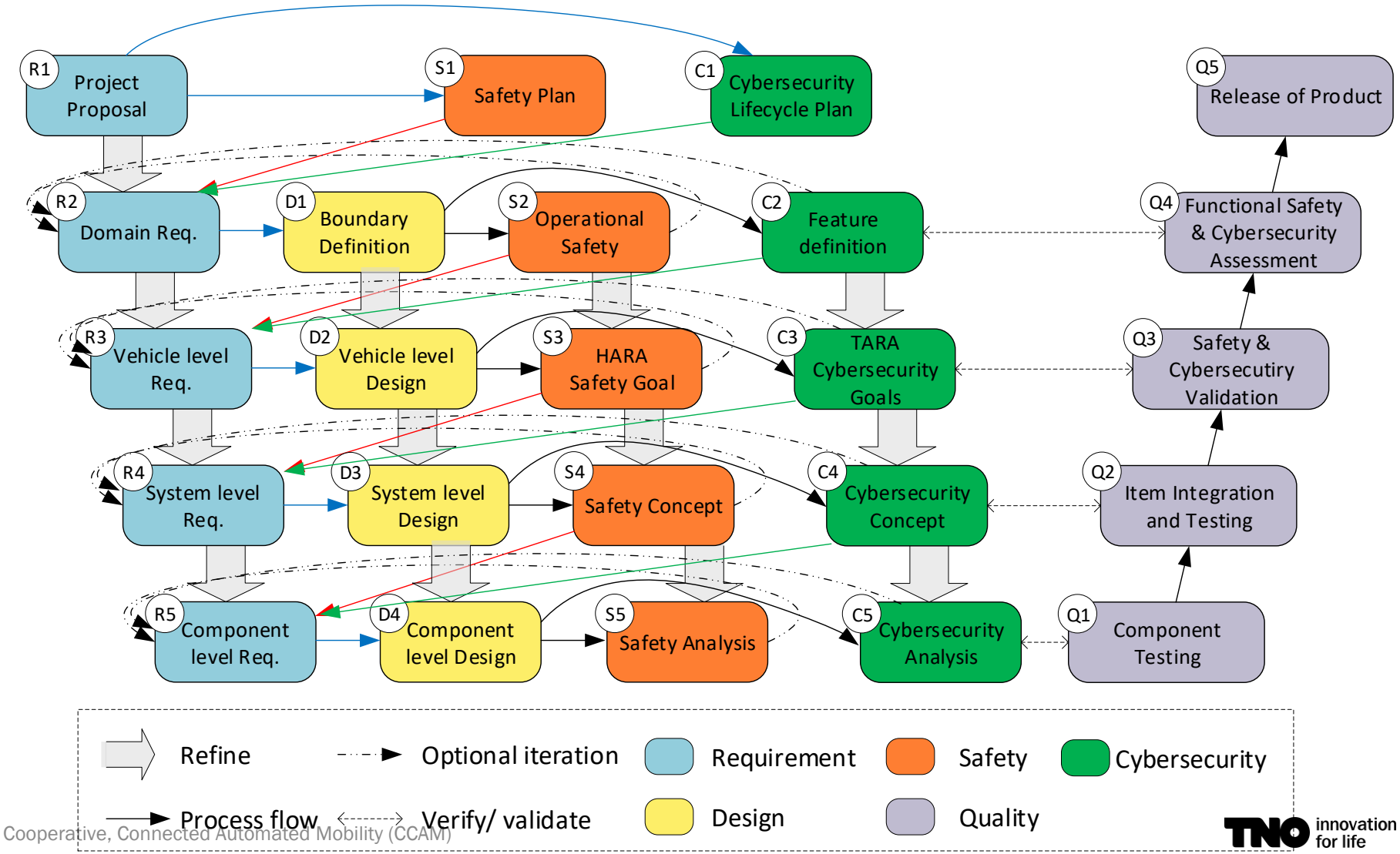
ENABLING METHODOLOGIES

- Integrated safety & security assessment methods
- Digital Twins
- Digital sovereignty
- Model-Based Systems Engineering

TECHNOLOGIES

SYSTEM DEVELOPMENT PROCESS

- V-cycle



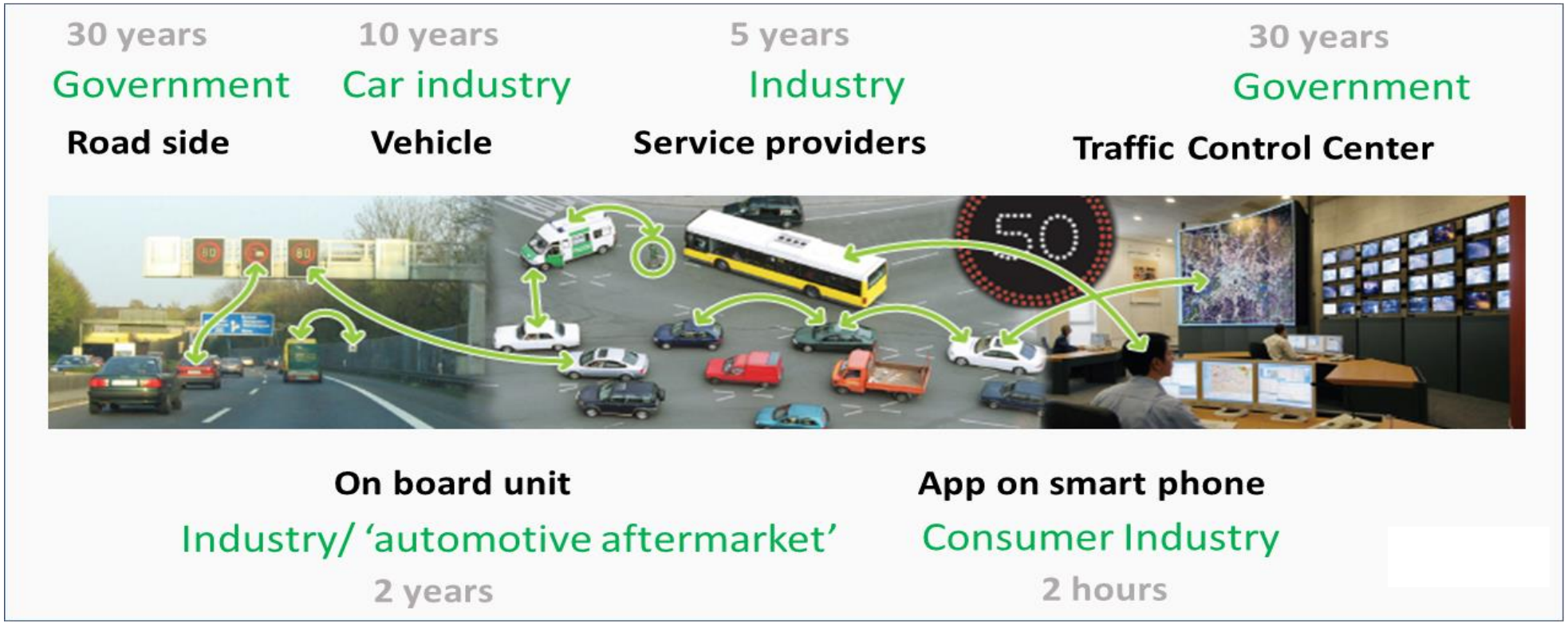
CHALLENGES – SAFETY RELATED
TOPICS

- Stakeholders
- Process
- Technical

CHALLENGES – SAFETY RELATED
MULTI-STAKEHOLDERS

- How to ensure safety for “conventional” and automated traffic?
- How to handle an up-to-date multi-stakeholder safety assurance?

- …many system components
- …with different owners,
- …and different life cycles



CHALLENGES – SAFETY RELATED
PROCESS

- Complex systems (or system-of-systems) require different development approaches
- Systems-of-systems are much more complicated to Verify & Validate (V&V) → certification & standardisation
  - Continuous integration/update & testing
  - Digital Twins for testing
  - Facilities for real-life testing (including generation of other traffic participants & infrastructure)
- Consistency and version management is crucial → life-time configuration management of system parts and continues (over-the-air) updates required
  - Approval/certification processes after updates should be standardised
  - Dependencies between components should be managed very accurately
- Trust in the shared information (from external parties) needs to be regulated
- Run-time monitoring becomes essential → black box recorders

CHALLENGES – SAFETY RELATED
TECHNICAL

- How to define/develop safe architectures that can be support during the whole life-cycle?
- Which run-time monitoring is required for assurance → black box recorders for which (extendable) data?
- How to make interface flexible but still reliable and safe?
- How to balance the conflicting requirements between functionality, safety, and security?
  - Use of more shared sensors data → higher performance, more safety challenges (dependencies), larger attack surface
  - Standardisation of protocols & interfaces → faster acceptance and interoperability, easier safety assessment, easier to attack and larger impact
  - Strict more reliable encryption → more latency and less performance, higher safety, better security

CHALLENGES – SECURITY RELATED
TOPICS

- Stakeholders
- Process
- Technical

CHALLENGES – CYBER SECURITY RELATED
STAKEHOLDERS

- How to get all stakeholders aligned?
- How to solve responsibility of stakeholders?
- How to solve General Data Protection Regulation (GDPR) issues (related to sharing privacy information)?

CHALLENGES – CYBER SECURITY RELATED
PROCESS

- How to regulate the trust in the shared information?
  - Multiple parties/stakeholders are involved in providing the data
  - Multiple parties/stakeholders need to support the security and protocols of communication channels
- How to create safe and secure software bug fixes/updates at a short notice to solve/mitigate the cyber attacks?
- How to ensure cyber security during the whole life-cycle (e.g. 15 years)?
  - Which organisational structure needs to created after the first official release?
  - How to support ethical hacking to find vulnerabilities?
  - How to share vulnerabilities?
  - What to do with vehicle/infrastructure that do not update after new releases?
- Which organisational structure is required to support the integrated (transdisciplinary) approach to develop safe & secure systems?
- How to regain trust after being attacked?

CHALLENGES – CYBER SECURITY RELATED
TECHNICAL

- How to detect attacks in the (local/global) networks?
- How to distinguish anomalies between faults and attacks?
- How to mitigate effects of attacks (robustness & resilience):
  - How to isolate the attack (where it is initiated)?
  - How to react → what is the safe state (e.g. automated parking along the road)?
  - How to safe and securely share attack information in the network (to limit the effects of the complete traffic flow)?
- Which (own and shared) data needs to be stored for analysing cyber attacks?
- Which post-quantum cryptography algorithms and protocols needs to be developed?
- How to make secure electronic components, interfaces, operating systems, firmware, communication, software and tooling?
- How to handle General Data Protection Regulation (GDPR) while attacks need to be analysed?

CONCLUSIONS
MANY CHALLENGES

TRUST

- Trust in the CCAM system-of-systems is crucial to get people to use and pay for these system

MULTIDISCIPLINARY AND TRANSDISCIPLINARY

- System-of-systems thinking is required to get these systems operational and keep them Safe & Secure

STANDARDISATION & REGULATION & POLICY

- Still many standards need to be developed and regulations needs to be approved to get the automated system to be approved by road authorities
- Harmonisation of validation methods are required
- Industry standards for architectures and infrastructure are required
- Life-time interoperability of system-of-systems and services is challenging


TNO innovation for life
QUESTIONS?